

УДК 343.3/7



© **Алексей Ульянов**
 професор кафедри тактико-спеціальної та вогневої підготовки Одеського державного університету внутрішніх справ (Україна), кандидат юридичних наук, доцент

© **Aleksey Ulyanov**
 Professor of the tactical-special and fire training dept. of the Odessa State University of Internal Affairs (Ukraine), PhD in Law, Associate Professor
 e-mail: v1976t@ukr.net



© **Олександр Ніколасв**
 доцент кафедри тактико-спеціальної та вогневої підготовки Одеського державного університету внутрішніх справ (Україна), кандидат політичних наук, доцент

© **Oleksandr Nikolayev**
 Associate professor the tactical-special and fire training dept. of the Odessa State University of Internal Affairs (Ukraine), PhD in Political Sciences, Associate Professor
 e-mail: v1976t@ukr.net



© **Вячеслав Ташматов**
 доцент кафедри тактико-спеціальної та вогневої підготовки Одеського державного університету внутрішніх справ (Україна), кандидат політичних наук

© **Vyacheslav Tashmatov**
 Associate professor of the tactical-special and fire training dept. of the Odessa State University of Internal Affairs (Ukraine), PhD in Psychology
 e-mail: v1976t@ukr.net

ПРАВОВЕ РЕГУЛЮВАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Стаття присвячена питанням правового регулювання протидії кіберзлочинності в Україні. Розкрито доктринальні підходи до визначення таких понять як: «кіберзлочинність», «кіберпростір», «злочини у сфері комп'ютерної інформації». Проведено аналіз міжнародно-правових актів та законодавства України у сфері боротьби з кіберзлочинністю, зроблено висновок про необхідність удо-

сконалення національного законодавства та налагодження плідної міжнародної співпраці у сфері розроблення механізмів протидії кіберзлочинності та мінімізації її негативних наслідків.

Впровадження та розвиток інформаційно-телекомунікаційних технологій сприяло формуванню кібернетичного простору, який впливаючи на політичне, соціально-економічне становище актуалізує необхідність забезпечення кібербезпеки, адже саме кіберзлочинність, на думку науковців, становить сьогодні найбільшу загрозу як для кожної держави окремо, так і для всієї міжнародної спільноти.

В Стратегії кібербезпеки України зазначено, що переваги сучасного цифрового світу та розвиток інформаційних технологій обумовили виникнення нових загроз національній та міжнародній безпеці. Поряд із інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб [1].

Для успішної боротьби з кіберзлочинністю, як явищем динамічним, деструктивним, по своїй суті антисоціальним, актуальним є вдосконалення засад правового регулювання боротьби в зазначеній сфері.

Питанню правового регулювання кібербезпеки, протидії кіберзлочинності наукові дослідження присвятили такі науковці як: В. Л. Бурячок, В. Б. Дзюндзюк, І. В. Діордіца, Д. В. Дубов, О. В. Манжай, Ю. М. Онищенко, О. В. Орлов, П. І. Пушкаренко та інші. Разом з тим, питання правового регулювання боротьби з кіберзлочинністю в Україні потребують додаткового узагальнення та висвітлення з урахуванням положень міжнародно-правових актів, які регулюють правовідносини в зазначеній сфері, що вказує на актуальність та своєчасність проведеного авторами наукового дослідження у форматі наукової статті.

Слід зазначити, що питання пов'язані з кіберзлочинністю досліджуються науковцями у різних аспектах.

С. А. Буяджи у дисертаційному дослідженні за темою: «Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект», значну увагу приділив генезису правового регулювання боротьби з кіберзлочинністю в світі та Україні. Внаслідок аналізу правової доктрини автором виділено чотири етапи процесу розвитку явища кіберзлочинності.

До першого етапу автор відносить підготовчий етап який охоплює кінець 60-х років — початок 70-х років ХХ століття, що є початковим моментом вчинення злочинів із використанням електронних обчислювальних машин.

Другий етап — розповсюдження кіберзлочинності, який охоплює початок 70-х років XX століття — 1986 рік) — ознаменувався початком появи хакерів та їх організованих груп, а завершився із прийняттям першого в історії нормативно-правового акту, присвяченого кіберзлочинам та першого в історії арешту хакера;

Третій етап автор визначає як етап транснаціональних кіберзлочинів та кібертероризму (1994 рік — початок XXI століття) .

Четвертий етап — сучасний етап кіберзлочинності (XXI століття) — етап появи нових форм комп'ютерних злочинів.

На нашу думку автор слушно доходить висновку, що генезис розвитку кіберзлочинності та генезис правового регулювання боротьби з кіберзлочинністю не можна ототожнювати. Кіберзлочинність розвивається у відповідності з еволюцією новітніх технологій, тому на сьогоднішній день є сферою, яка постійно на крок попереду її нормативно-правового регулювання [2].

Дану позицію підтримують Є. В. Коваленко та О. В. Плетньов, які звертаючи увагу на те, що кіберзлочинність має дуже високий потенціал розвитку та підвищення своєї негативної ефективності, зазначають невідповідність швидкості розвитку засобів злочинної діяльності у кіберпросторі швидкості законодавчого врегулювання та впровадження тих або інших засобів протидії такій діяльності [3, с. 59].

І. В. Діордіца, досліджуючи питання щодо змісту кіберзагроз на сучасному етапі, доходить висновку про те, що неналежне правове регулювання в національному кібернетичному просторі України призводить до низки негативних явищ, які створюють реальні та потенційні загрози кібернетичній безпеці. У зв'язку з чим, автор акцентує увагу на необхідності розроблення науково обґрунтованої державної політики в цій галузі, визначення системи національних цінностей, життєво важливих інтересів особистості, суспільства та держави, визначення зовнішніх і внутрішніх загроз цим інтересам, пошуку ефективних заходів для забезпечення безпеки в усіх її сферах, захисту від інформаційних загроз і реалізації права на отримання достовірної інформації [4, с. 101].

Правові засади боротьби і протидії кібертероризму можна розділити на два відповідних взаємопов'язаних рівня:

1. Міжнародно-правові акти, підписані та ратифіковані Україною.
2. Національне законодавство України.

До міжнародно-правових актів, що регулюють боротьбу з кіберзлочинністю можна віднести Конвенцію про кіберзлочинність від 23.11.2001 року [5], яка ратифікована Верховною Радою України

07.09.2005 року і є єдиним юридично обов'язковим міжнародним документом з кібербезпеки, який встановлює спільну кримінальну політику щодо захисту від кіберзлочинності шляхом прийняття відповідного внутрішнього законодавства та сприяння міжнародному співробітництву.

Конвенція не надає визначення кіберзлочинності хоча в її преамбулі зазначено, що Конвенція є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку.

Для виконання Будапештської Конвенції Ради Європи про кіберзлочинність, Указом Президента України від 15.03.2016 року була затверджена Стратегія кібербезпеки України, метою якої є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Для досягнення зазначеної мети Стратегією передбачено проведення наступних заходів:

- створення національної системи кібербезпеки;

- посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері;

- забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура).

В стратегії визначаються пріоритетні напрями забезпечення кібербезпеки України серед яких чільне місце посідає завдання щодо створення вітчизняної нормативно-правової та термінологічної бази у цій сфері, гармонізації нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки відповідно до міжнародних стандартів і стандартів ЄС та НАТО.

Стратегія стала джерелом для розроблення нормативно-правових актів з питань кібербезпеки.

У 2017 році було прийнято Закон України «Про основні засади забезпечення кібербезпеки України» [6], який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини

і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

На законодавчому рівні визначено такі поняття як: кібербезпека, кіберзагроза, кіберзлочин, кіберзлочинність, кіберпростір та ін.

Відповідно до закону кібербезпека визначається як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

В свою чергу кіберпростір визначається як середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та / або інших глобальних мереж передачі даних;

Визначаючи поняття кіберзлочину, законодавець ототожнює його з поняттям комп'ютерного злочину, зазначаючи, що кіберзлочин (комп'ютерний злочин) — суспільно небезпечне винне діяння у кіберпросторі та / або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та / або яке визнано злочином міжнародними договорами України.

Дане визначення не є безспірним. Підходи щодо визначення співвідношення зазначених категорій різні як серед науковців так і на рівні тлумачних словників.

На думку В. М. Бутузова комп'ютерні злочини та кіберзлочини є різними видами злочинів у сфері високих інформаційних технологій, класифікація яких відбувається за такими ознаками: — ознакою віднесення певних злочинів до комп'ютерних є знаряддя вчинення злочину — комп'ютерна техніка. Автор зазначає, що об'єктом посягання є суспільні відносини у сфері автоматизованої обробки інформації; — ознакою віднесення злочинів до кіберзлочинів є специфічне середовище вчинення злочинів — кіберпростір (середовище комп'ютерних систем та мереж). При цьому автор посилається на перелік протиправних діянь, які передбачені в Конвенції та Додатковому протоколі до неї. На його думку, тільки діяння із цього переліку можуть бути віднесені до кіберзлочинів [7, с. 5–6].

Ю. А. Бельський зазначає, що кіберзлочини це злочини, які вчиняються в процесі автоматизованої обробки інформації за допомогою електронно-обчислювальних машин або через комп'ютерні системи, об'єктом посягання яких є суспільні відносини у сфері обігу електронної інформації та інші суспільних відносин, у яких комп'ютер виступає кваліфікуючою ознакою вчинення злочину (наприклад, комп'ютерне шахрайство, або кібертероризм) [8, с. 417]. О. К. Копатін та Є. Д. Скулишин визначають кіберзлочин як злочин, пов'язаний із використанням кібернетичних комп'ютерних систем, та злочин у кіберпросторі. На відміну від комп'ютерного злочину, поняття якого пов'язане з використанням будь-якої комп'ютерної техніки, кіберзлочин є більш вузьким поняттям, пов'язаним із функціонуванням саме кібернетичних комп'ютерних систем [9, с. 85–86].

І. В. Діордіца зазначає, що термін «кіберзлочинність» часто вживається поряд з терміном «комп'ютерна злочинність», причому нерідко ці поняття використовуються як синоніми. Автор погоджуючись з тим, що ці терміни дуже близькі один одному, вважає їх не синонімічними, зазначаючи при цьому, що поняття «кіберзлочинність» (в англійському варіанті — *cybercrime*) ширше, ніж «комп'ютерна злочинність» (*computer crime*), і більш точно відображає природу такого явища, як злочинність в інформаційному просторі. Свою точку зору аргументує визначеннями Оксфордського тлумачного словника, який визначає приставку «*cyber*» як компонент складного слова. Її значення — що відноситься до інформаційних технологій, мережі Інтернет, віртуальної реальності. Практично таке ж визначення дає Кембриджський словник. Таким чином, «*cybercrime*» — це злочинність, пов'язана як із використанням комп'ютерів, так і з використанням інформаційних технологій і глобальних мереж. У той же час термін «*computer crime*» в основному стосується злочинів, які скоєні щодо комп'ютерів або комп'ютерних даних. Ідея поділу термінів «кіберзлочинність» і «комп'ютерна злочинність» й використанню саме першого терміну і закріплена в міжнародному праві. Рада Європи в листопаді 2001 року прийняла Конвенцію про кіберзлочинність, вживши саме термін «*cybercrime*», а не «*computer crime*» [4].

Наомість А. А. Музика та Д. С. Азаров визначають тотожність понять «кіберзлочини» та «злочини у сфері комп'ютерної інформації». Вчені наголошують, що визначити кіберзлочин необхідно, як злочин у сфері комп'ютерної інформації [10, с. 5].

Л. В. Сорока також дотримується визначення комп'ютерні злочини, відповідно до якого — це злочини, у яких комп'ютер безпосередньо

є предметом та (або) зняряддям здійснення правопорушень у суспільних сферах, які пов'язані з використанням комп'ютерної техніки [11, с. 263].

Проведений аналіз доктринальних підходів свідчить, що серед науковців немає одностайності у визначенні кіберзлочину, що обумовлено різним трактування кіберпростору та способів використання комп'ютерних систем у вчиненні відповідних неправомірних дій.

Попри розбіжності у науковій доктрині постає питання також співвідношення міжнародного законодавства та законодавства України щодо визначення переліку незаконних дій, які віднесено до злочинів, вчинених у кіберсфері.

Висновки. Отже, кіберзлочинність є порівняно новим видом суспільно небезпечних діянь.

Відповідно до Конвенції правопорушення розподілені на чотири групи.

До першої групи входять правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем.

До другої групи входять правопорушення пов'язані з комп'ютерами.

Третю групу складають злочини, пов'язані з контентом (змістом).

До четвертої групи увійшли порушення авторського права і суміжних прав.

В Кримінальному кодексі України не вживається категорія кіберпростір та кіберзлочин, разом з тим, встановлена відповідальність за скоєння злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку) [12].

Статті Конвенції	Статті КК України	Розділи КК України
Ст. 2. Незаконний доступ	Ст.ст. 361, 363	Розділ XV
Ст. 3. Нелегальне перехоплення	Ст.ст. 163, 359, ч. 2 ст. 362,	Розділ V, Розділ XV
Ст. 4. Втручання у дані	Ст.ст. 361, 362, 363-1	Розділ XV
Ст. 5. Втручання в систему	Ст.ст. 361, 361-1, 362, 363, 363-1	Розділ XV
Ст. 6. Зловживання пристроями	Ст.ст. 361, 362, 363	Розділ XV
Ст. 7. Підробка, пов'язана з комп'ютерами	Ст. 200	Розділ VII
Ст. 8. Шахрайство, пов'язане з комп'ютерами	Ст. 190 ч. 3	Розділ VI
Ст. 9. Правопорушення пов'язані з дитячою порнографією	Ст. 301	Розділ XII
Ст. 10. Правопорушення, пов'язані з порушенням авторських та суміжних прав	Ст. 176	Розділ V

Виходячи з наведеної таблиці, в Кримінальному кодексі України злочини пов'язані з використанням комп'ютерних, інформаційних технологій, крім розділу XV закріплені також в інших розділах кодексу.

Слід зазначити, що 28.01.2003 р. було затверджено додатковий протокол до Конвенції про кіберзлочинність з метою введення кримінальної відповідальності за правопорушення, пов'язані з проявом расизму та ксенофобії, які здійснюються з використанням комп'ютерних систем, а саме:

- стаття 3 «Поширення расистського та ксенофобного матеріалу через комп'ютерні системи»;
 - стаття 4 «Погроза з расистських та ксенофобних мотивів»;
 - стаття 5 «Образ з расистських та ксенофобних мотивів»;
 - стаття 6 «Заперечення, значна мінімізація, схвалення або виправдання геноциду чи злочинів проти людства» [13].
- Аналіз зазначених статей дає змогу зробити висновок про те, що кваліфікуючою ознакою здійснення кожного з перелічених злочинів є застосуванням комп'ютерних мереж. Стосовно правопорушень передбачених ст. 3–5 додаткового протоколу, Кримінальний кодекс України статтею 161 передбачає відповідальність за порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками, не зазначаючи при цьому, що такий злочин вчиняється із застосуванням комп'ютерних мереж.

Що стосується статті шостої додаткового протоколу щодо правопорушень пов'язаних з геноцидом чи злочинів проти людства, то в КК України статтею 442 передбачена відповідальність за геноцид. Даний злочин також не віднесений до злочинів, які вчиняються з використанням комп'ютерних, інформаційних технологій.

Таким чином проведений порівняльний аналіз положень Міжнародної Конвенції та Кримінального кодексу України свідчить, що переважна більшість злочинів, пов'язаних з використанням комп'ютерних технологій, отримали відповідне регулювання в національному законодавстві. Разом з тим, окремі злочини, попри їх законодавче регулювання, не виділяють використання комп'ютерних, інформаційних технологій, як спеціальний спосіб їх вчинення.

Стрімкий розвиток інформаційно-технологічних систем буде завжди випереджати законодавче регулювання відносин в цій сфері, в тому числі й обумовлюючи потребу в оновленні переліку неправомірних дій, за які має наставати кримінальна відповідальність.

Попри те, що у наукових дослідженнях, присвячених питанням боротьби з кіберзлочинами, провідною є позиція фахівців щодо необхідності удоскона-

лення законодавства у зазначеній сфері та приведення його у відповідність до міжнародних стандартів, що є беззаперечно слушним, все ж таки для протистояння кіберзлочинності цього не достатньо. Поряд з законодавчим забезпеченням має бути налагоджена плідна міжнародна співпраця у сфері розроблення механізмів протидії кіберзлочинності та мінімізації її негативних наслідків, оскільки кіберзлочинність не залежить від кордонів, а мережа Інтернет відкриває безмежні можливості для злочинців з усього світу. Що обумовлює важливість проведення подальших наукових розробок питань протидії кіберзлочинності як на національному, так і міжнародному рівні.

Список основних джерел

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс] : Указ Президента України, 15 березня 2016 року № 96/2016. — Режим доступу: <https://zakon5.rada.gov.ua/laws/show/96/2016>. — Дата доступу: 05.03.2020.

2. Буяджи, С. А. Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект : дис. ... канд. юрид. наук : 12.00.01 / С. А. Буяджи. — Київ, 2018. — 203 л.

3. Коваленко, Є. В. Передумови загроз у сфері інформаційної безпеки та перспективи їх подолання / Є. В. Коваленко, О. В. Плетньов // Актуальні проблеми управління інформаційною безпекою України : зб. тез наук. доповідей X Всеукраїнська наук.-практ. конф., Київ, 4 квітня 2019 року / Нац. акад. СБУ. — Київ, 2019. — С. 57–61.

4. Діордіца, І. В. Поняття і зміст кіберзагроз на сучасному етапі / І. В. Діордіца // Підприємництво, господарство і право. — 2017. — № 4. — С. 99–107.

5. Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 р. // Офіційний вісник України. — 2007. — № 65. — Ст. 2535.

6. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] : Закон України, 5 жовтня 2017 р. — Режим доступу: <https://zakon.rada.gov.ua/laws/show/2163-19>. — Дата доступу: 05.03.2020.

7. Амелін, О. Визначення кіберзлочинів у національному законодавстві / О. Амелін // Науковий часопис Національної академії прокуратури України. — 3'2016. — С. 1–6.

8. Бельський, Ю. А. Щодо визначення поняття кіберзлочину / Ю. А. Бельський // Юридичний вісник. — 2014. — Вип. № 6. — С. 414–418.

9. Копатін, О. Словник термінів з кібербезпеки / О. Копатін, Є. Скулишин. — Київ : ВБ «Аванпост-Прим», 2012. — 214 с.

10. Лісовий, В. В. «Комп'ютерні» злочини: питання кваліфікації / В. В. Лісовий // Право України. — 2002. — Вип. № 2. — С. 86–89.

11. Сорока, Л. В. Види правопорушень у сфері комп'ютерних та інформаційних технологій / Л. В. Сорока // Наукові записки КДПУ. Сер. Історичні науки. — Кіровоград : КДПУ ім. В. Винниченка, 2005. — Вип. 9. — С. 262–270.

12. Кримінальний кодекс України 5 квітня 2001 року [Електронний ресурс]. — Режим доступу: <https://zakon.rada.gov.ua/laws/show/2341-14>. — Дата доступу: 03.03.2020.

13. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи [Електронний ресурс]. — Режим доступу: http://zakon.rada.gov.ua/laws/show/994_687. — Дата доступу: 05.03.2020.

Legal regulation of combating cybercrime in Ukraine

The article is devoted to the legal regulation of combating cybercrime in Ukraine. The doctrinal approaches to the definition of such concepts as: “cybercrime”, “cyberspace”, “crime in the field of computer information” are disclosed. The analysis of international legal acts and legislation of Ukraine in the field of combating cybercrime is made, the conclusion is drawn on the need to improve national legislation and establish international cooperation in the development of mechanisms to counter cybercrime and minimize its negative consequences. Crimes provided for in the Convention are enshrined in different chapters of the Criminal Code of Ukraine. It is indicated that the use of computer technologies as a way of committing them is not allocated for all crimes in the Code.

Правовое регулирование противодействия киберпреступности в Украине

Статья посвящена вопросам правового регулирования противодействия киберпреступности в Украине. Проведен анализ доктринальных подходов к определению и соотношению таких понятий, как «киберпреступность», «киберпространство», «преступления в сфере компьютерной информации», на основании которого сделан вывод о том, что единого мнения как в определении вышеуказанных понятий, так и их соотношения не существует. Сформировано три подхода к соотношению данных категорий: первый — «киберпреступность» шире понятия «преступления в сфере компьютерной информации», второй — «преступления в сфере компьютерной информации» шире понятия киберпреступности, третий — это тождественные категории. Такая ситуация обусловлена разной трактовкой категорий «киберпространство» и «способ использования компьютерных систем при совершении соответствующих неправомерных деяний».

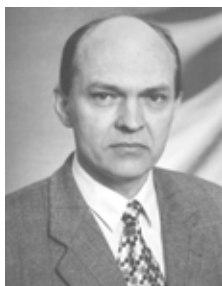
Проанализированы международно-правовые акты и законодательство Украины в сфере борьбы с киберпреступностью. Международно-правовым актом, сыгравшим значительную роль в развитии законодательства Украины, является Конвенция о киберпреступности от 23.11.2001 года, которая устанавливает общую уголовную политику по защите от киберпреступности, предусматривающую принятие соответствующего внутреннего законодательства и содействие международному сотрудничеству.

Среди нормативно-правовых актов Украины, регулирующих вопросы борьбы с киберпреступностью, отмечены Стратегия кибербезопасности Украины 2016 года и Закон «Об основных принципах обеспечения кибербезопасности Украины» 2017 года, который стал основой развития государственной системы защиты в указанной сфере.

Подавляющее большинство преступлений, связанных с использованием компьютерных технологий, предусмотренных Конвенцией и Протоколом к Конвенции от 28.01.2003 года, получили соответствующее регулирование в Уголовном

кодексе Украины. Вместе с тем отдельные преступления, несмотря на их законодательное регулирование (например, нарушение равноправия граждан в зависимости от их расовой, национальной принадлежности, религиозных убеждений, инвалидности и по другим признакам (ст. 161 УК Украины), геноцид (ст. 442 УК Украины)), не выделяют использование компьютерных, информационных технологий как специальный способ их совершения.

УДК 37.0



© **Александр Федоров**

профессор кафедры педагогики и социокультурного развития личности Ростовского государственного экономического университета (Россия), доктор педагогических наук, профессор

© **Alexander Fedorov**

Professor of the sociocultural development of the personality dept. of the Rostov State University of Economics (Russia), Doctor of Pedagogy, Professor e-mail: 1954alex@mail.ru



© **Анастасия Левицкая**

проректор по научной работе Таганрогского института управления и экономики (Россия), кандидат педагогических наук, доцент

© **Anastasia Levitskaya**

Vice-rector for scientific work of the Taganrog Institute of management and economics (Russia), PhD in Pedagogics, Associate Professor e-mail: a.levitskaya@tmei.ru

ТЕОРЕТИЧЕСКИЕ МОДЕЛИ И ТЕОРИИ МЕДИАОБРАЗОВАНИЯ В СТРАНАХ СНГ¹

Контент-анализ диссертаций по тематике медиаобразования, защищенных в СССР, России и странах СНГ с 1960 по 2019 год, показал, что вплоть до начала XXI века наблюдался паритет между практико-утилитарными и

¹ Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (РФФИ) в рамках научного проекта № 18-013-00022 «Массовое медиаобразование в странах СНГ (1992—2020)». Руководитель проекта — профессор А. В. Федоров.